2N PICard Commander

Manuel d'installation

2N TELEKOMUNIKACE a.s.
Modřanská 621 | Prague 4 | 143 01

2N.com

Table des matières

Symboles et termes utilisés

Les symboles et pictogrammes suivants sont utilisés dans le manuel :

DANGER
Toujours se conformer ces instructions pour éviter tout risque de blessure.

AVERTISSEMENT
Toujours se conformer ces instructions pour éviter d'endommager l'appareil.

ATTENTION
Avertissement important. Le non-respect des instructions peut entraîner un dysfonctionnement de l'appareil.

ASTUCE
Informations utiles pour une utilisation ou une configuration plus facile et plus rapide.

NOTE
Procédures et conseils pour une utilisation efficace des fonctionnalités de l'appareil.

Description du produit

2N PICard Commander est une application logicielle permettant de crypter les informations d'identification sur les cartes d'accès. L'application crée des projets qui génèrent un ensemble de clés de chiffrement et de lecture. Les clés du lecteur de projet peuvent être importées dans les appareils 2N ou dans **Access Commander**, qui assure ensuite la distribution des clés de lecture aux appareils 2N connectés.

La technologie **2N PICard** est conçue pour le cryptage des cartes **MIFARE DESFire EV2** et **MIFARE DESFire EV3**.

Dans l'application **PICard Commander** il est possible de supprimer les données enregistrées sur les cartes d'accès.

Fonctionnalités de l'application **PICard Commander** est soumis à l’achat d’une licence.

Produits connexes

2N Part No. 91379601

Axis Part No. 02722-001

Licence de commandant 2N PICard

La licence est toujours délivrée pour un lecteur de carte USB spécifique en fonction de la clé de périphérique du lecteur donné. Les lecteurs de clé de périphérique peuvent être trouvés avant de télécharger la licence dans **PICard Commander**. Les lecteurs de cartes USB pris en charge sont répertoriés ci-dessous.

2N Part No. 9137421E

Axis Part No. 01400-001

Lecteur USB de cartes RFID 13,56 MHz, 125 kHz et appareils NFC/HCE

Lecteur de carte RFID externe pour connexion au PC via interface USB. Convient pour la gestion du système et l'ajout de cartes 13,56 MHz, 125 kHz et d'appareils Android avec prise en charge NFC/HCE via l'interface Web ou l'application d'interphone IP 2N **Commandant d'accès**. Convient pour télécharger des cartes MIFARE DESFire vers une application de cryptage **PICard Commander**[a.]. Il lit les mêmes types de cartes et d'appareils que les lecteurs de cartes des interphones IP 2N :

Cartes RFID prises en charge 125 kHz :

- EM4x02
- NXP HiTag2

Cartes RFID prises en charge 13,56 MHz :

- **ISO14443A** (MIFARE Classic, MIFARE Plus, MIFARE Mini, MIFARE Ultralight, MIFARE DESFire CSN only)
- **PicoPass** (HID iClass CSN, Picopass)
- **FeliCa** (Standard, Lite)
- **ST SR** (SR, SRI, SRIX)
- **My2N**
- **2N PICard**

2N Part No. 9137424E

Axis Part No. 01527-001

Sécurisé Lecteur USB de cartes RFID 13,56 MHz, 125 kHz et appareils NFC/HCE

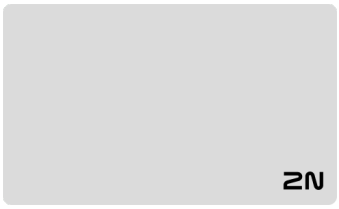
Lecteur de carte RFID externe sécurisé pour connexion au PC via interface USB. Convient pour la gestion du système et l'ajout de cartes 13,56 MHz, 125 kHz et d'appareils Android avec prise en charge NFC/HCE via l'interface Web ou l'application d'interphone IP 2N **Access Comander**. Convient pour télécharger des cartes MIFARE DESFire vers une application de cryptage **Commande PICard** année[a]. Il lit les mêmes types de cartes et d'appareils que les lecteurs de cartes des interphones IP 2N :

125 kHz

- EM4xxx
- HID Prox

13,56 MHz

- ISO14443A (MIFARE DESFire)
- PicoPass (HID iClass)
- FeliCa
- ST SR(IX)
- My2N
- HID SE (Seos, iClass SE, MIFARE SE)



2N Part No. 11202601

Axis Part No. 02787-001

Carte RFID 2N MIFARE Desfire EV3 4K 13,56MH 10 pièces

paquet de 10 pièces

MIFARE DESFire EV3 (ISO14443A)

2N Part No. 11202602

Axis Part No. 02788-001

Porte-clés RFID 2N MIFARE Desfire EV3 4K 13,56 MHz 10 pièces

paquet de 10 pièces

MIFARE DESFire EV3 (ISO14443A)

[a] Technologie **2N PICard** est destiné au cryptage des cartes MIFARE DESFireEV2 et MIFARE DESFire EV3.

Appareils compatibles

La technologie de lecture PICard est prise en charge par tous les lecteurs RFID 2N lancés en février 2023 ou plus tard. La plupart des lecteurs fabriqués après cette date sont également compatibles, à l'exception des modèles énumérés ci-dessous.

Les modèles suivants **ne sont pas compatibles**:

- **2N IP Base**: tous les lecteurs RFID
- **2N IP Force**: 9151011, 9151012, 9151016, 9151017, 9151019
- **2N IP Vario**: tous les lecteurs RFID
- **2N IP Verso**: 915503x, 915504x, 915508x
- **2N Access Unit M**: 91611x
- **2N Access Unit 1.0**: 916008, 916009, 916010, 916011, 916013, 916016, 916019
- **2N Access Unit 2.0**: 916033x

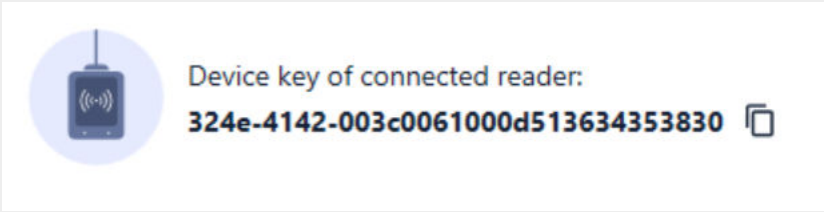
Pour les modules suivants, la compatibilité n'est garantie que pour les unités fabriquées à l'automne 2023 ou plus tard :

- **2N IP Force**: 9151031, 9151031S

Installation et chargement des licences

1. Installez-le **PICard Commander** de la manière habituelle via le programme d'installation.
2. Après avoir lancé l'application, chargez la licence en cliquant sur Load License dans la barre orange (ou sous **Help > License**). Chargez ensuite le fichier de licence à partir du disque. Le lecteur de cartes doit être connecté à l'ordinateur pour pouvoir charger la licence.

NOTE
La licence est liée à un lecteur de carte USB spécifique. Pour obtenir une licence, vous devez spécifier la clé du lecteur, qui peut être trouvée dans les informations de licence de **PICard Commander** (onglet **Help > License**). Le lecteur de carte doit être connecté à l'ordinateur pour visualiser la clé.



Connecter un autre lecteur

Si un lecteur autre que celui associé à la licence que vous utilisez est connecté à votre ordinateur, **PICard Commander** vous alertera lorsqu'il démarrera. Sous **Help > License**, vous pouvez télécharger une nouvelle licence.

Projet

La création de projets individuels permet de chiffrer des groupes de cartes d'accès dans différents modes. Vous pouvez configurer chaque projet spécifiquement dans le but d'utiliser les cartes. Le projet génère une série de clés de chiffrement et de lecture. Vers l'appareil ou vers **Access Comander** vous pouvez télécharger les clés de lecture d'un seul projet à la fois.

Créer un nouveau projet

Après avoir ouvert l'application, appuyez sur le bouton pour créer un nouveau projet **Start new project**.

Chemin alternatif : onglet **File > New project**

Un nouvel assistant de configuration de projet s'ouvrira, suivez les étapes ci-dessous Paramètres du projet (p. 9).

Ouverture du projet

1. Dans l'interface initiale de l'application, cliquez sur le bouton Open project.
   Itinéraire alternatif : **File > Open project**

Les projets ouverts les plus récemment sont affichés dans la partie inférieure de l'interface initiale de l'application.

Paramètres du projet

Au démarrage d'un projet, il est nécessaire de définir ses paramètres.

Les paramètres peuvent être modifiés ultérieurement dans la configuration du projet dans l'interface initiale de l'application (autre chemin : onglet **Project > Change configuration**).

Paramètres de base (Basic Settings)

- **Project name** – nom du projet
- **Project description** – espace pour saisir des notes sur le projet

Clé de chiffrement principale (Main Encryption Key)

En fonction de la clé de chiffrement principale (MEK), **2N PICard Commander** génère un ensemble de clés de chiffrement. La clé doit donc être unique et suffisamment sûre. Le jeu de clés est basé sur la clé de chiffrement principale, de sorte que les projets ayant la même clé de chiffrement principale génèrent les mêmes jeux de clés. Si un projet est perdu, un nouveau projet doté de la même clé de chiffrement principale peut être créé et poursuivre le chiffrement.

AVERTISSEMENT
La clé de cryptage principale ne peut pas être ultérieure **voir ou modifier**.

ASTUCE
Pour une sécurité maximale, il est important de sauvegarder à la fois le fichier de projet lui-même et la clé de cryptage principale (MEK). Il est idéal de stocker la clé de cryptage principale (MEK) en toute sécurité loin de l'environnement en ligne, par exemple dans un coffre-fort, etc.

Mode de cryptage (Card mode)

Il est possible de choisir parmi les modes de cryptage de carte suivants :

- **Card may be used for other applications later on (best compatibility)** – Les cartes seront principalement utilisées par les systèmes 2N. Les données de la carte seront cryptées, mais son UID restera lisible par des applications tierces. Les cartes peuvent être reformatées dans leur état d'origine.
- **Card will be used only for access control with 2N devices (best privacy)** – Les cartes seront utilisées exclusivement dans les systèmes 2N. Les paramètres de la carte seront définitivement réinitialisés. Une fois cryptée, la fonction Random ID est activée sur la carte.
- **Card is already used for other applications (advance settings)** – Des applications tierces sont déjà chargées sur les cartes. À l'étape suivante, vous pouvez définir les paramètres sélectionnés des cartes MIFARE DESFire dont la technologie possède les données d'accès **2N PICard** à chiffrer dans le projet.

NOTE
Sélection de mode **Card is already used for other applications** est irréversible.

À l'étape suivante, vous pouvez remplir :

- **Application ID (AID)** – le code sous lequel la candidature sera déposée **2N PICard** identifié sur la carte. AID est préréglé sur 53324E.
- **PICC master key type** – le type de clé principale PICC définie sur les cartes dont dispose l'application **2N Picard** Crypter.
- PICC master key – la valeur des cartes maîtresses PICC dont dispose l'application **2N PICard** Crypter.
- **Enable randomisation of readable card ID** – l'activation de la fonction Random ID garantit que l'UID de la carte change de manière aléatoire à chaque chargement. Ainsi, une personne non autorisée ne peut pas utiliser la carte à mauvais escient pour identifier son titulaire.
- **Encrypt cards in factory default state (change default PICC master key)** – option permettant de télécharger la clé principale PICC spécifiée sur d'autres cartes vierges lors de leur chiffrement dans le projet. Si cette option n'est pas sélectionnée, **PICard Commander** refusera de chiffrer une carte vide.

AVERTISSEMENT

- Après le processus de cryptage de la carte sous le nouvel AID, vous devez réexporter les clés de lecture. Les cartes précédemment cryptées avec l'ancien AID deviendront illisibles pour l'appareil 2N.
- En changeant la clé principale PICC dans un projet avec des cartes déjà cryptées, il sera impossible de modifier ces cartes plus loin dans le projet et de supprimer leurs données. La validité des cartes d'authentification dans le dispositif 2N ne sera pas affectée.
- L'activation de la fonction de carte d'identité aléatoire est irréversible. L'UID original de la carte reste illisible même après le formatage de la carte.

Enregistrer sur le disque

Le fichier de projet est enregistré sur le disque sous *Nom du projet*.picprj.

Cochez la case **Protect project file with password** pour définir un mot de passe de protection pour l'ouverture du projet. Le mot de passe peut être modifié ultérieurement dans l'onglet **záložce Project > Change protection password**.

AVERTISSEMENT
Vous ne pouvez pas oublier votre mot de passe plus tard **afficher ou restaurer**.

Cryptage et lecture de cartes

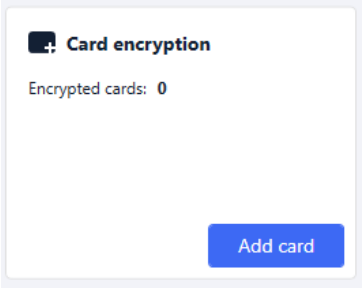
Voici un aperçu de ce que vous trouverez dans le chapitre :

Cryptage de la carte

Le processus de cryptage des cartes dans **PICard Commander** attribue à chaque carte un identifiant unique de 128 bits, qui est ensuite crypté à l'aide des clés de cryptage du projet respectif. Dans le projet, il est possible de charger la carte et ainsi connaître son identifiant attribué, éventuellement d'autres informations sur la carte et s'il est possible de la crypter dans le projet.

Processus de cryptage

1. Dans l'interface initiale de l'application, cliquez sur **Add card** dans la rubrique **Card encryption**.
   Chemin alternatif : onglet **Project > Encrypt New Card**

   Credential ID for new card – nouvel identifiant de la carte téléchargée
2. Placez la carte sur le lecteur. En appuyant sur le bouton **Encrypt** les données d'accès sont attribuées à la carte, qui sont en même temps cryptées.

   ASTUCE
   En cochant la case à droite, vous pouvez lancer le cryptage automatique des autres cartes attachées sans avoir à appuyer à nouveau sur le bouton **Encrypt**.
3. L'application informe du cryptage réussi de la carte.

Si la carte n'a pas pu être cryptée, l'application en informe la raison :

- **Card cannot be encrypted** - application **PICard Commander** n'a pas accès à la carte-clé principale PICC. Si vous souhaitez chiffrer des cartes avec une clé principale PICC prédéfinie, vous devez sélectionner le mode de chiffrement approprié dans Paramètres du projet (p. 9).
- **Not enough free space on card** – il n'y a pas assez d'espace sur la carte pour télécharger la technologie **2N PICard**. La mémoire minimale requise est de 512 B.
- **Unsupported card** – l'application ne prend pas en charge ce type de carte. Technologie **2N PICard** est conçu pour crypter les cartes MIFARE DESFire EV2 et EV3.
- **Only MIFARE DESFire EV2 or EV3 are supported** – l'application ne prend pas en charge ce type de carte. La carte chargée est MIFARE DESFire EV1.
- **Communication failure with card** – le lecteur n'a pas réussi à lire la carte. Placez la carte contre le lecteur et ne la retirez pas tant que le processus de cryptage n'est pas terminé

ASTUCE
Dans la partie inférieure de la fenêtre se trouve une liste déroulante d'identifiants de carte cryptés. Si vous souhaitez enregistrer la liste, copiez-la avant de fermer la fenêtre. La fermeture de la fenêtre supprime la liste. Plus tard, les identifiants ne pourront être affichés que pour des cartes individuelles.

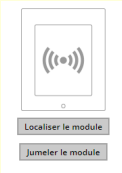
Export des clés de lecture

Pour que les appareils 2N puissent accéder aux données des cartes cryptées, ils doivent connaître les clés de lecture du projet. À partir de **PICard Commander**, les clés de lecture peuvent être exportées vers un appareil 2N ou vers **Access Commander**, qui assure la distribution à tous les appareils 2N connectés. Une fois les clés de lecture téléchargées vers les appareils, ces derniers seront également en mesure de lire les cartes qui ont été cryptées dans le projet après le téléchargement des clés de lecture.

1. Cliquez sur Export dans la section Reader keys export de l'interface d'accueil de l'application (chemin alternatif : onglet **Project > Export reader keys**).
2. Vous pouvez exporter les clés du lecteur de projet de deux manières :

   - Exporter les clés vers un fichier (p. 13)
   - Téléchargez les clés vers **Access Comander** (p. 14)

ATTENTION
Si vous venez de connecter un module d'extension de lecteur de cartes RFID à l'appareil 2N à l'aide d'un câble VBUS, vous devez coupler ce module avec l'appareil. Le couplage du module d'extension de lecteur s'effectue via l'interface Web de l'appareil dans la section Matériel, dans le menu Modules d'extension.

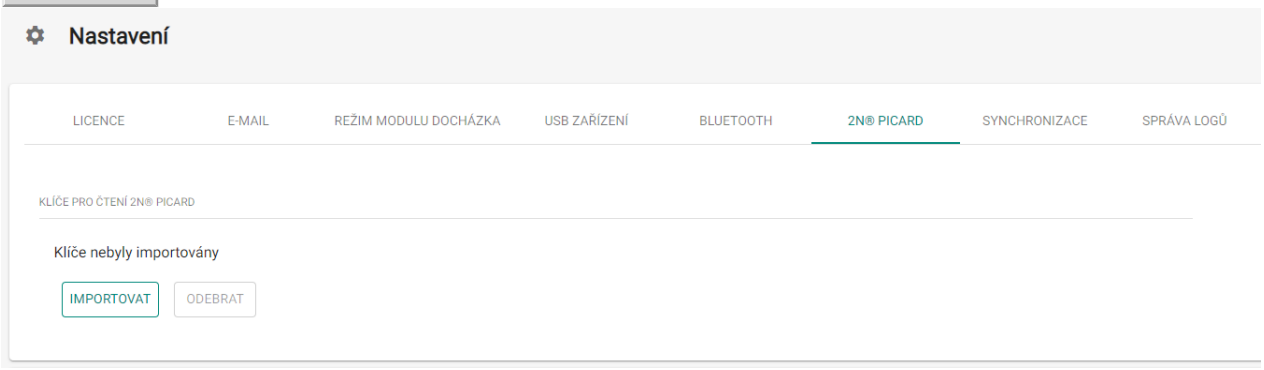


Exporter les clés vers un fichier

L'application génère un fichier de clé et l'enregistre sur le disque. Le fichier doit ensuite être importé dans les paramètres de l'appareil 2N ou dans **Access Comander** via leurs interfaces Web. À l'étape suivante de l'exportation, il est possible de définir un mot de passe pour le fichier enregistré.

- **Importation dans Access Commander (version 3.00 et supérieure)** via l'interface web : **Paramètres > Accès > Onglet Clés PICard >** Importation

- **Importer dans Access Commander** via l'interface web : **Paramètres système > 2N PICARD > rubrique** IMPORTER



- **Importer vers un appareil 2N** via l'interface web :

Téléchargez les clés vers Access Comander

Application **PICard Commander** télécharge les clés de lecture directement sur **Access Comander**, qui assure une distribution ultérieure aux appareils 2N connectés. À l'étape suivante, il est nécessaire de saisir les données de connexion de l'administrateur pour la licence. **Access Comander**.

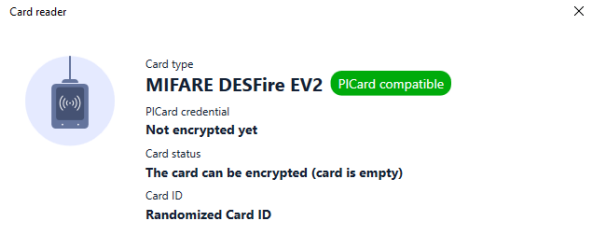
Adresse – Adresse HTTP de l'interface web **Access Comander**

Login name – nom de connexion du compte administrateur **Access Commanderu**

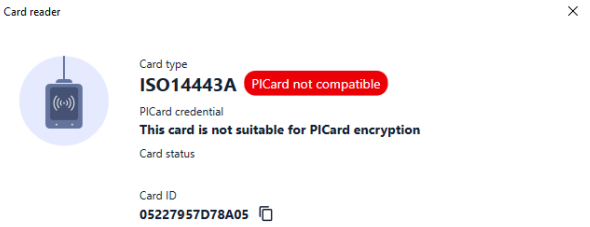
Password– mot de passe de connexion pour le compte donné **Access Commanderu**

Lire les informations de la carte

Vous pouvez consulter l'identifiant de la carte et d'autres informations sur la carte et ses options de cryptage dans l'onglet **Project > Read card**. Les informations sont lues lorsque la carte est insérée dans le lecteur.



Cette carte peut être cryptée dans l'application.



Ce type de carte ne peut pas être crypté dans l'application.

PICard credential nrécupère l'identifiant de la carte attribué lors du processus de cryptage. Si la carte ne possède pas d'identifiant, des informations sur ses options d'attribution apparaîtront :

- **Not encryptable** – le type de carte est compatible avec la technologie **2N PICard**, mais le projet n'a pas accès à sa clé principale PICC.
- **This card is not suitable for PICard encryption** – l'application ne prend pas en charge ce type de carte. Technologie **2N PICard** est destiné au cryptage des cartes MIFARE DESFire EV2 et EV3.
- **Not encrypted yet** – la carte peut être cryptée.
- **Unknown** – la carte est cryptée dans un autre projet sous une clé de cryptage principale différente. La carte peut également être endommagée.

Card Status affiche l'état ou les options de cryptage de la carte donnée :

- **Valid PICard credential** – la carte est cryptée dans ce projet.
- **The card can be encrypted (card is empty)** – la carte n'est pas cryptée. Il y a des paramètres d'usine sur la carte.
- **The card can be encrypted** – la carte n'est pas cryptée. Une clé principale PICC compatible avec ce projet est définie sur la carte.
- **Different PICC Master Key detected. Card's current PICC Master Key required for encryption** – la carte ne peut pas être cryptée dans ce projet. La clé principale PICC définie est différente.
- **PICard application created in a different project, so cannot be read in this project**– la carte est cryptée dans un autre projet.
- **Only MIFARE DESFire EV2 or EV3 are supported** – la carte ne peut pas être cryptée. L'application ne prend pas en charge ce type de carte. La carte chargée est MIFARE DESFire EV1.
- **INVALID CREDENTIAL (there's a problem with the digital signature)** – les données d'accès cryptées de la carte ne peuvent pas être affichées. Leur authenticité n'a pu être confirmée. La signature numérique n'est pas valide.

Card ID affiche l'UUID de la carte ou signale que la fonction Random ID est activée.

Effacer les données de la carte

Application **PICard Commander** permet de formater les cartes ou d'effacer leurs données d'accès cryptées. Les cartes ne peuvent être supprimées et formatées que dans le projet dans lequel elles sont cryptées.

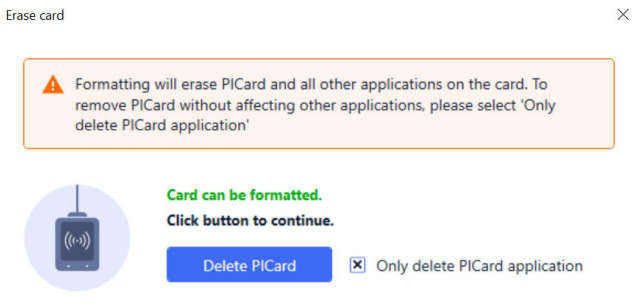
Formatage de la carte

AVERTISSEMENT
Le formatage de la carte effacera toutes les données de la carte, y compris les données tierces.

1. Ouvrez l'onglet **Project > Format Card**.
2. Fixez la carte sur le lecteur. Appuyez sur le bouton Format card pour formater la carte.

NOTE
Si la fonction Random ID est activée sur la carte, le formatage de la carte ne restaurera pas la lisibilité de l'UID d'origine.

Supprimer les données d'accès



1. Ouvrez l'onglet **Project > Format Card**.
2. Cochez la case **Only delete PICard application**.
3. Placez la carte contre le lecteur.

4. En appuyant sur le bouton Delete PICard les données d'accès cryptées de la carte seront supprimées.

Licences tierces

Une liste complète des licences de bibliothèques tierces utilisées est fournie dans l'onglet **Help > About**.

2N PICard Commander – Manuel d'installation

2N.com